PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

# FORENSIC ANALYSIS WORKSHEET

| | | | |
|---|---|---|---|
| Agency Case #: | PA2017-249357 | Lab #: | CF-17-00087 |
| Date Received: | 3/27/2017 | Requesting Officer: | Trooper Barton Josefowicz |
| Requesting County: | Lehigh | Requesting Agency: | Pennsylvania State Police |
| Received By: | J. Langton | Analyst(s): | Jonathan D. Langton |
| Search Warrant: | Yes | Consent Form: | N/A |

## SUMMARY

The requesting agency is investigating a sex offense and requested forensic analysis of digital evidence obtained during the investigation.

The investigator(s) specifically requested extraction of digital artifacts related to but not limited to the following data:

Information related to digital device usage, user information, electronic communications, call logs, event logs, text/chat messages, website & Internet history, search history, image & video files and GPS/location data.

The extracted artifacts may assist with the investigation.

Information provided by investigator(s) to assist with the analysis:

[OPTIONAL FIELD]

| Subject Name | Subject Type | Device Association | Item # Association |
|---|---|---|---|
| Zhinin, Sandro | Accused | Owner/User | F1, F2, G1 |
| Subject Name | Subject Type | Device Association | Item # Association |
| [redacted] | Victim | N/A | N/A |
| Subject Name | Subject Type | Device Association | Item # Association |
| | | | |
| Subject Name | Subject Type | Device Association | Item # Association |
| | | | |
| Subject Name | Subject Type | Device Association | Item # Association |
| | | | |

[OPTIONAL FIELD]

| | |
|---|---|
| Location: | Hanover Township |



Jonathan D. Langton

Exhibit 2

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

## EVIDENCE SUBMITTED

See Attachment – Request for Forensic Analysis Form.

## ACTION TAKEN

3/27/2017

Digital items were submitted to the Petzold Digital Forensic Lab on a Request for Forensic Analysis Form. A lab number of CF-17-00087 was assigned. All evidence submitted on the lab request for forensic services form was examined and/or analyzed. Digital forensic methods & procedures were used to examine all evidence. A summary of the forensic methods and examination results is listed below.

## SOFTWARE/HARDWARE TOOLS UTILIZED (Checked):

| | |
|---|---|
| Document Solutions, Inc USB Write Blocker | ☐ |
| Tableau Ultrablock II – Model T35es (Write Block Device) | ☐ |
| Tableau T35689iu Forensic Bridge (Write Block Device) | ☐ |
| Forensic Series AFT EX-S3 Memory Card Reader | ☐ |
| Guidance Software EnCase | ☐ |
| Access Data Registry Viewer | ☐ |
| Access Data FTK Imager | ☐ |
| Cellebrite UFED 4PC | ☒ |
| Cellebrite Physical Analyzer | ☒ |
| Cellebrite Write Block Forensic Memory Card Reader | ☐ |
| Cellebrite Cloud Analyzer | ☒ |
| Tableau TD2u Forensic Duplicator | ☐ |
| Magnet Forensics Internet Evidence Finder (IEF) | ☐ |
| None/Not Applicable | ☐ |
| Other | ☐ |



Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

# FORENSIC DETAILS

| DEVICE INFORMATION [The *examiner* determines which data blocks are optional or relevant to the examination] | | | | |
|---|---|---|---|---|
| **Item Number:** | F1 | | | |
| **Type Device:** | Cell Phone | | | |
| **Manufacturer:** | Apple | | | |
| **Model:** | iPhone A1533 | | | |
| **Mobile Device Identifier:** | IMEI | 013971006138041 | | |
| **SIM Card:** | Yes. See Extraction Report for ICCID Number | | | |
| **Memory Card Slot:** | No | **Size:** | N/A | |
| **Passcode/Password Protection:** | Passcode | **Value:** | Unknown | |
| **Damage to Device:** | No | | | |
| **System Date/Time:** | N/A | **Actual Date/Time:** | N/A | |
| **Exam Complete:** | Partial. Device passcode protected. | **Date of Exam:** | 3/30/2017 | |
| **Type of Exam:** | Logical Extraction of SIM Card Data | | | |

| DEVICE INFORMATION [The *examiner* determines which data blocks are optional or relevant to the examination] | | | | |
|---|---|---|---|---|
| **Item Number:** | F2 | | | |
| **Type Device:** | Tablet | | | |
| **Manufacturer:** | LG | | | |
| **Model:** | V495 | | | |
| **Serial Number:** | 604CQDG320482 | | | |
| **Mobile Device Identifier:** | IMEI | 358169063204821 | | |
| **SIM Card:** | No | | | |
| **Memory Card Slot:** | N/A | **Size:** | N/A | |
| **Passcode/Password Protection:** | N/A | **Value:** | N/A | |
| **Damage to Device:** | Yes. Explain | Device Screen Cracked | | |
| **System Date/Time:** | N/A | **Actual Date/Time:** | N/A | |
| **Exam Complete:** | Yes. Successfully. | **Date of Exam:** | 3/27/2017 | |
| **Type of Exam:** | Physical Extraction of Mobile Device | | | |



Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

| DEVICE INFORMATION [The examiner determines which data blocks are optional or relevant to the examination] | | | | |
|---|---|---|---|---|
| **Item Number:** | G1 | | | |
| **Type Device:** | Cell Phone | | | |
| **Manufacturer:** | Google | | | |
| **Model:** | G-2PW4100 Pixel | | | |
| **SIM Card:** | Yes. See Extraction Report for ICCID Number | | | |
| **Memory Card Slot:** | N/A | **Size:** | N/A | |
| **Passcode/Password Protection:** | Passcode | **Value:** | Unknown | |
| **Damage to Device:** | No | | | |
| **System Date/Time:** | N/A | **Actual Date/Time:** | N/A | |
| **Exam Complete:** | Partial. Device passcode protected. | **Date of Exam:** | 3/30/2017 | |
| **Type of Exam:** | Logical Extraction of SIM Card Data | | | |

## RESULTS

**Evidentiary Items of Interest Discovered:** Yes. See Extraction Report(s)

**Additional Information**:

***Item #F2: LG V495 Tablet***

One (1) video file of interest was located during the examination of the LG V495 Tablet. The video file of interest appears to display sexual activity in a hotel room, as detailed in the investigator's affidavit of probable cause, and can be located in the global extraction report under "Tags". In addition to the video file of interest, four (4) Skype instant message conversations of interest were located, including what appears to be a possible conversation with the alleged victim. These conversations can be located in the global extraction report, and were also exported and attached as individual sub-reports.

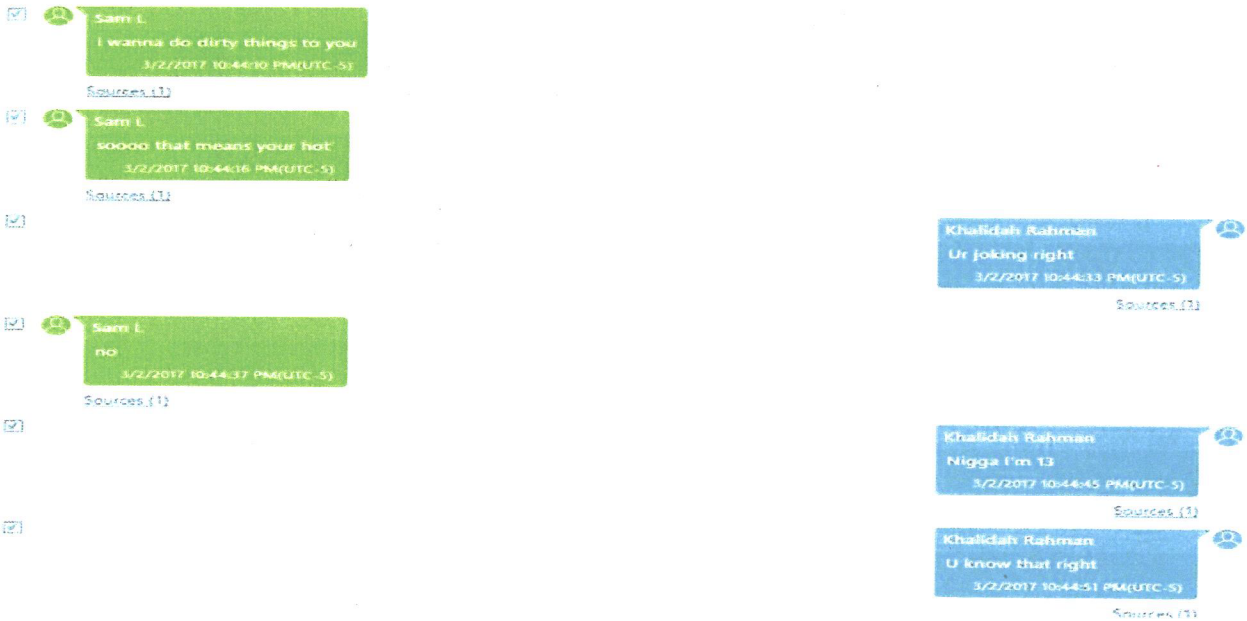
The following screenshot depicts a Skype instant message conversation between a user named [redacted]" with the display name of "I should just fucking die", who appears to be the alleged victim, and the end user of the LG V495 tablet, using the Skype username "sam.l016", with the display name of "Sam L" on 3/4/2017:



Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547


The following screenshots depict a Skype instant message conversation between the end user of the LG V495 tablet, using the Skype username "sam.l016", with the display name of "Sam L", and a possible juvenile using the Skype username "[redacted]", with the display name of [redacted] [redacted]" on 3/2/2017:

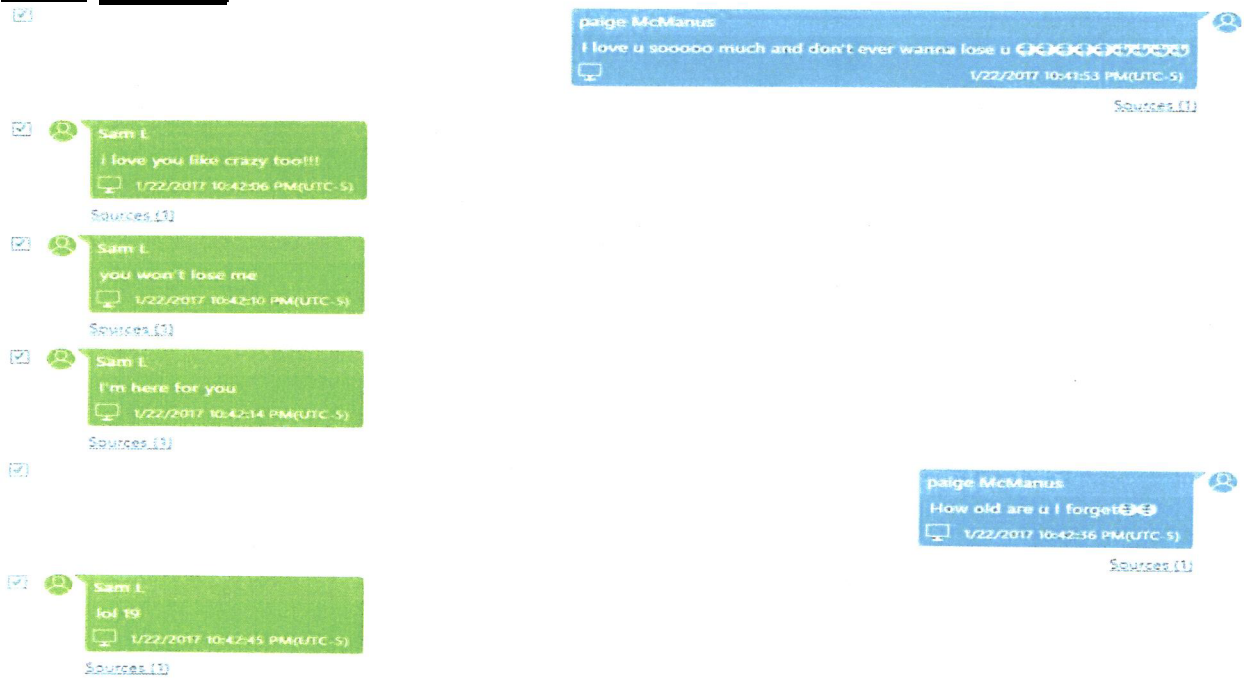





Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547


The following screenshot depicts a Skype instant message conversation between the end user of the LG V495 tablet, using the Skype username "sam.l016", with the display name of "Sam L", and a possible juvenile using the Skype username [redacted]", with the display name of [redacted]" on 1/22/2017:

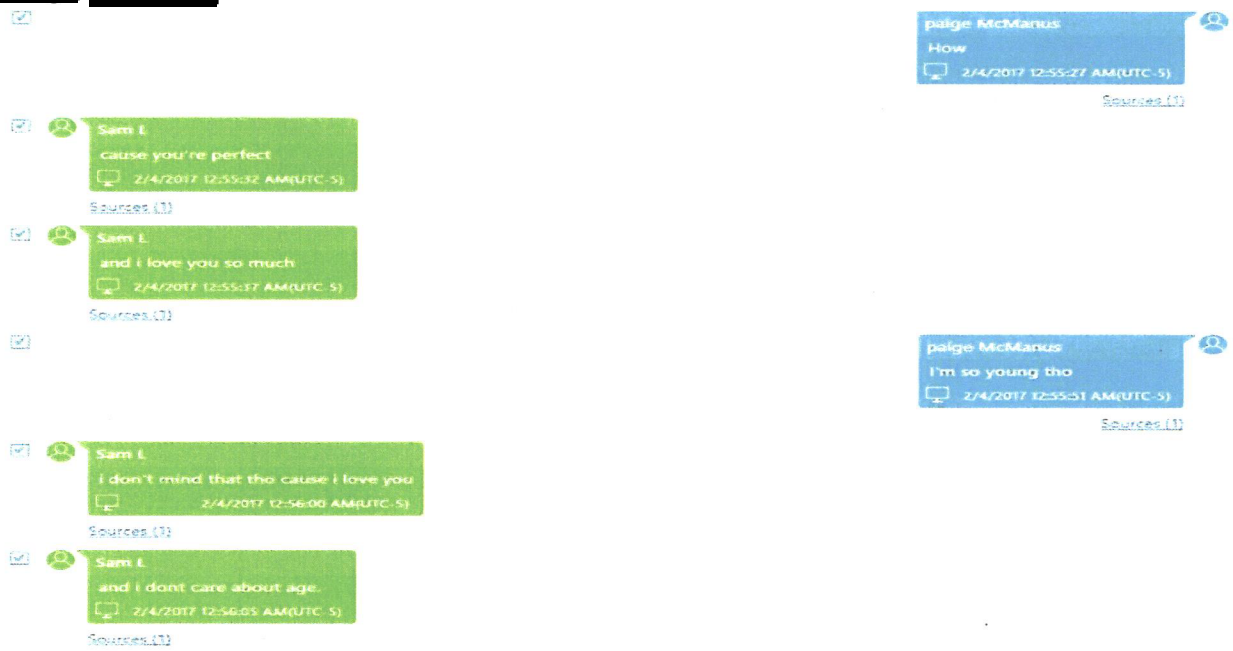




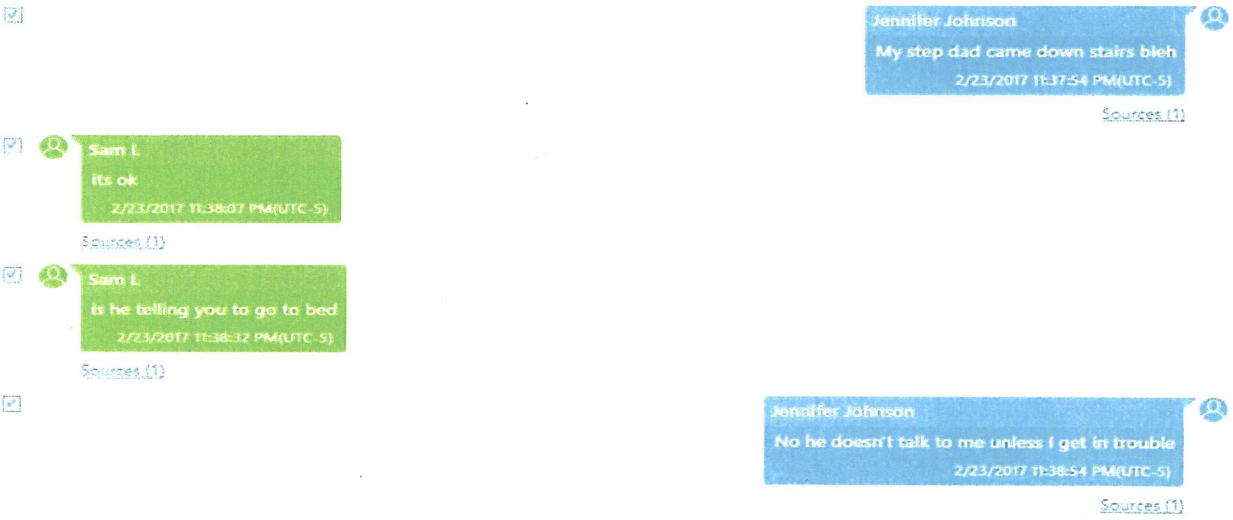

Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

The following screenshot depicts a Skype instant message conversation between the end user of the LG V495 tablet, using the Skype username "sam.l016", with the display name of "Sam L", and a possible juvenile using the Skype username [redacted]", with the display name of [redacted]" on 2/4/2017:




The following screenshot depicts a Skype instant message conversation between the end user of the LG V495 tablet, using the Skype username "sam.l016", with the display name of "Sam L", and a possible juvenile using the Skype username [redacted]", with the display name of [redacted]" on 2/23/2017:

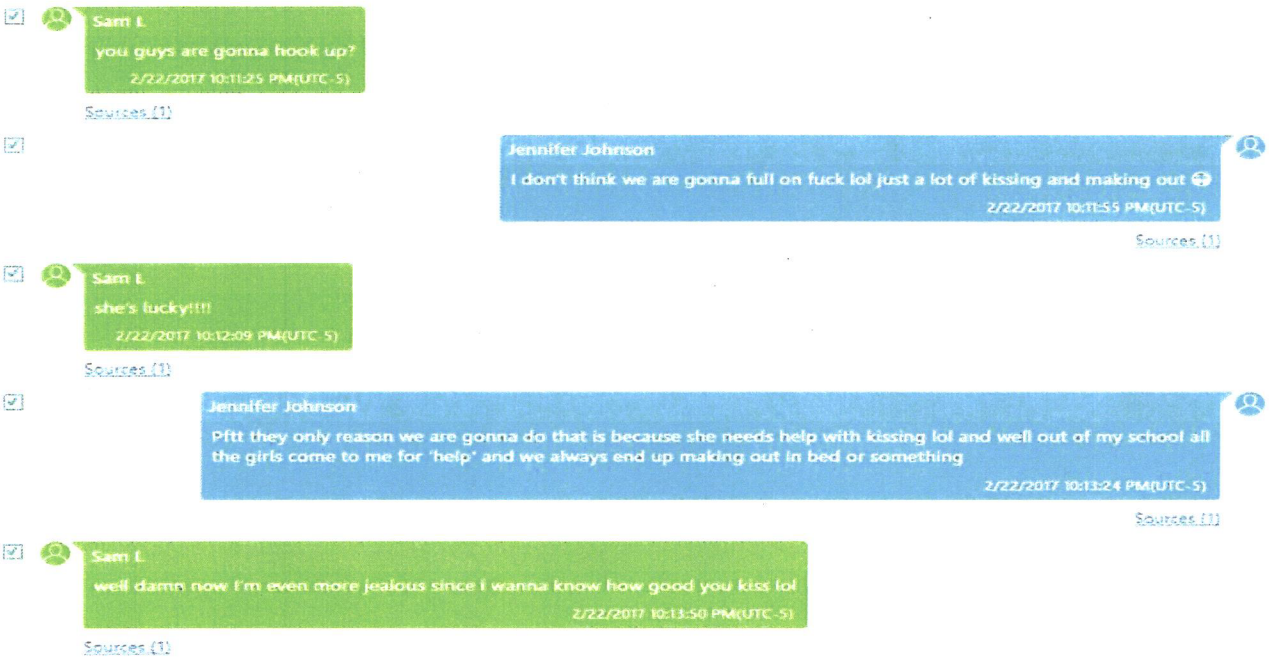





Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

The following screenshot depicts a Skype instant message conversation between the end user of the LG V495 tablet, using the Skype username "sam.l016", with the display name of "Sam L", and a possible juvenile using the Skype username "[redacted]", with the display name of "[redacted]" on 2/22/2017:




Additionally, remotely stored digital artifacts from a Google user account were subsequently acquired through the utilization of Cellebrite Cloud Analyzer. Data was acquired from the following account:

Google: Sandro Zhinin (szhinin@gmail.com)

A report was generated that contains the acquired data, which has been saved to external media. Three (3) Google internet history artifacts of interest can be located in the global Cloud Analyzer Report, and are excerpted below:

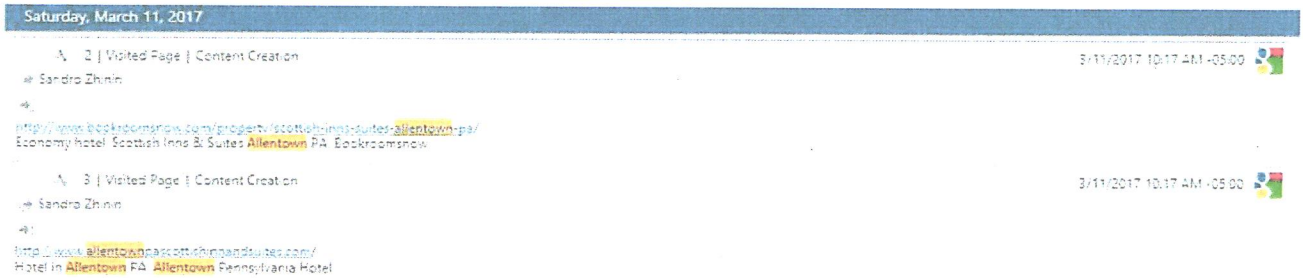
The following screenshot depicts one (1) Google internet history artifact pertaining to the Red Roof Inn on 3/4/2017:




Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

The following screenshot depicts two (2) Google internet history artifacts pertaining to the Scottish Inn on 3/11/2017:




## CONCLUSION/RECOMMENDATION

Extraction Reports were created: Yes. Saved to external media.

It is recommended the investigator(s) review the extraction report(s) for artifacts of evidentiary value.

All items of evidence were returned to the investigating agency.



Jonathan D. Langton

PETZOLD DIGITAL FORENSIC LAB
2755 Station Ave., Center Valley, PA 18034
Phone 610.282.2547

## SUMMARY FORENSIC METHODS & DEFINITIONS

Digital Forensic Procedures are followed to preserve original evidence and to prevent the altering or changing of any data. Digital evidence is protected during the forensic examination process by utilizing hardware and/or software write blocking methods/procedures. For example, a hard disk drive is attached to a computer forensic recovery device via a write block device and is then forensically previewed and/or imaged (acquired). During the acquisition process, a bit-for-bit image is created – including allocated files, unallocated space (including erased files), slack space (including disk, volume and random access memory [RAM] slack), and unused disk space. Disk and volume slack is the space between the logical end and the physical end of a file (EOF), or disk, or volume where deleted files and text fragments may be recovered. RAM slack is the space from the end of the file to the end of the containing sector. After the acquisition process, the original digital device is returned to evidence. The image is then analyzed using one or more forensic software suite tools. Such as; Guidance Software EnCase Forensic Software, AccessData FTK (Forensic Tool Kit) and/or other forensic tools.

When processing mobile devices, a hardware extraction tool and/or software tools are utilized to assist in the recovery and interpretation of user data from the device. One such tool is Cellebrite's Universal Forensic Extraction Device (UFED). Depending on the device the following forensic methods are used for data extraction:

***Logical Extraction:*** extraction of data is performed through the device's application programming interface (API). Upon connection, UFED loads the API to the device. The API extracts data in a read only mode from the operating system. This process enables the acquisition of most of the live data in the device, in a readable format and forensically sound manner.

***Physical Extraction:*** provides a bit for bit copy of the entire flash memory of the device. This method enables the acquisition of live data, hidden and/or deleted data. Customized boot loaders (small program) that includes read only functionality are used to extract data.

***File System Extraction:*** acquisition of files (data) embedded in the memory of a device. This is a process of extracting data from the devices memory including images, videos, database files system files and logs. Most of the built in and user applications (apps) store their data in these database files.

***Global System for Mobile Telecommunications (GSM):*** Cellular network standard used by mobile devices around the world.

***International Mobile Equipment Identifier (IMEI):*** Unique number used to identify mobile devices using the GSM standard. It is typically 15 digits & structured into three parts. Type allocation code (TAC): first 8 digits - identifies the vendor & mode of the device. Serial Number (SN): 6 digits after TAC. Checksum: (Optional) Algorithm computed against the TAC & SN for authentication & to verify integrity of the IMEI.

***Subscriber Identification Module (SIM):*** Smart card used to identify & authenticate subscribers of mobile devices on the service provider network.

***Integrated Circuit Card Identifier (ICCID):*** 19 or 20 digit serial number that uniquely identifies a SIM card.

***International Mobile Subscriber Identifier (IMSI):*** 14 or 15 digit number that uniquely identifies the subscriber with a cellular network provider.

***Mobile Subscriber ISDN (MSISDN):*** 11 digit number used to reach the mobile device.

***Code Division Multiple Access (CDMA):*** Cellular network standard used by mobile devices.

***Mobile Equipment Identifier (MEID):*** Unique number (15 digit Hex number) used to identify mobile devices using the CDMA standard.



Jonathan D. Langton